La regulación de los datos de tráfico en la Unión Europea

Perez Asinari, Maria Veronica

Published in:
Jurisprudencia Argentina

Publication date:
2004

Document Version
le PDF de l'éditeur

Este artículo fue publicado en *Jurisprudencia Argentina*, JA 2004-I, fascículo n. 4, Buenos Aires, 28 de abril de 2004, p. 49-59.

La regulación de los datos de tráfico en la Unión Europea. ¿Entre la seguridad y los derechos fundamentales?

María Verónica Pérez Asinari*

1. Introducción

La Unión Europea (UE) ha recientemente finalizado un proceso de reforma de la legislación comunitara en el ámbito de las comunicaciones electrónicas[1]. El resultado del mismo fue la sanción de seis Directivas y una serie de Decisiones y Recomendaciones[2], entre las cuales se encuentra la Directiva referente a la protección de la intimidad y los datos personales en este ámbito específico, Directiva 2002/58/CE[3].

---

* Investigadora en el *Centre de Recherches Informatique et Droit (CRID)*, *Facultés Universitaires Notre-Dame de la Paix*, Namur, Bélgica, veronica.perez@fundp.ac.be, http://www.droit.fundp.ac.be/crid/

Agradezco a Jean-Marc DINANT, investigador en el CRID, por las interesantes discusiones tenidas sobre determinados aspectos tecnológicos.

Este artículo se basa, en parte, en ciertos conceptos expresados en Sophie LOUVEAUX y María Verónica PEREZ ASINARI "New European Directive 2002/58 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector – Some Initial Remarks", *Computers and Telecommunications Law Review*, volume 9, issue 5, 2003, p. 133-138.

[1] European Commission, *The 1999 Communications Review*, DG INFSO, Directorate A. Septiembre 2000.

[2] Para una visión global de la reforma ver : Alexandre DE STREEL, Robert QUECK, y Philippe VERNET "Le nouveau cadre réglementaire européen des réseaux et services de communications électroniques", *Cahiers de droit européen*, 2002, N° 3-4, 243-314.

[3] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), *Diario Oficial n° L 201 de 31/07/2002 p. 0037 – 0047* (de aqui en adelante "la Directiva" o "la nueva Directiva"), disponible en:

La misma deroga la Directiva 97/66/CE[4] con el objeto de adaptarla al desarrollo de los mercados y de las tecnologías de los servicios de comunicaciones electrónicas de modo que el nivel de protección de la intimidad y de los datos personales sea el mismo independientemente de la tecnología utilizada. Es por ello que la nueva Directiva emplea un vocabulario "tecnológicamente neutral"[5], en la medida de lo posible, no sólo para hacerla aplicable a tecnologías que la Directiva 97/66/CE no cubriría "estrictamente", como es el caso de Internet[6], sino también para hacerla aplicable a futuros desarrollos tecnológicos[7].

Es importante señalar que la Directiva 2002/58/CE constituye *lex specialis*[8] *vis-à-vis* la Directiva 95/46/CE[9], con ello resultan directamente de aplicación las obligaciones del responsable del tratamiento y los derechos del titular de los datos en ella descriptos. No obstante, debemos tener en cuenta que la nueva Directiva hace extensiva su aplicación a "los

---

http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=es&numdoc=32002L0058&model=guichett

[4] Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, *Diario Oficial n° L 024 de 30/01/1998 p. 0001 – 0008*, disponible en: http://www.europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=es&numdoc=31997L0066&model=guichett

[5] El principio de neutralidad tecnológica se ve cristalizado en el Considerando 4 de la Directiva. "Ce principe vise tenir compte de la convergence et assure qu'aucune technologie n'est favorisée ou défavorisée par la réglementation. Ainsi, un service particulier doit être soumis au même régime, peu importe le type de réseau utilisé.", DE STREEL, QUECK, VERNET, *op. cit.*

[6] No obstante, el Grupo de Trabajo del Artículo 29 emitió una opinión favorable respecto de la aplicación de la Directiva 97/66/CE a Internet. Ver: *Privacy on the Internet-An integrated EU Approach to On-line Data Protection*, 21 noviembre 2000, WP37. A su vez, la Directiva 2000/31/CE sobre comercio electrónico reconoce expresamente la aplicabilidad de la Directiva 97/66/CE a los servicios de la sociedad de la información, tanto en su preámbulo como en su articulado (Considerandos 14 y 15, Artículos 1.5.b y 8.2).

[7] Sin embargo, una legislación tecnológicamente neutral que ignora las diferentes características y consecuencias de determinada tecnología puede ignorar también el diferente grado de violación a los derechos y garantías fundamentales que la misma puede conllevar, por lo tanto este principio no debe ser aplicado de manera absoluta. Ver: Ian HOSEIN y Alberto ESCUDERO PASCUAL "Understanding Traffic Data and Deconstructing Technology-neutral Regulations", disponible en: http://www.it.kth.se/~aep/publications/unece-latest-escuderoa-hoseini.pdf , última visita 07/07/03. Los autores exponen la siguiente opinión al respecto: "One reason for technology-neutral policy was a way to deal with the concerns of governments mandating a specific type or form of technology. While this is favourable in the development of some policies that affect market developments, e.g. to ensure choice and variability in the marketplace, technology-neutral lawful access policy is more problematic. Another reason for technology-neutrality is to ensure that new laws do not need to be passed every time a new technology is invented. Although it seems logical, this reasoning presented by policy-makers may be specious; one can not have the mandate of updating laws for new technologies then in the same breath argue against updating for the next new technology and thus require technology-neutral policy. It is our contention that technology-neutral language may be used to ignore, wilfull or not, the challenges, risks, and costs to applying powers to different technical infrastructures".

[8] Considerando 10 de la Directiva.

[9] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos *Diario Oficial n° L 281 de 23/11/1995 p. 0031 – 0050* (de aqui en adelante "la Directiva general"), disponible en http://www.europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=es&numdoc=31995L0046&model=guichett

intereses legítimos de las personas jurídicas"[10]. Lamentablemente no se define qué es lo que debe entenderse por "intereses legítimos", dejándolo a determinar por las leyes de transposición nacionales[11]. Tampoco es claro si, en tanto resulta una ampliación del ámbito de aplicación *ratione personae* de la Directiva 95/46/CE, son aplicables, respecto de las personas jurídicas, las obligaciones de los responsables del tratamiento y los derechos como titulares de datos descriptos en la Directiva general en toda su extensión.

El objeto de la nueva Directiva, como así también de la general es doble: (1) garantizar el respeto de los derechos fundamentales y observar los principios consagrados, en particular, en la Carta de los Derechos Fundamentales de la Unión Europea[12], específicamente los artículos 7[13] y 8[14] de dicha Carta, y la confidencialidad de las comunicaciones, de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales[15] y las constituciones de los Estados miembros; y (2) evitar obstáculos para el mercado interior en lo atinente a las comunicaciones electrónicas de conformidad con el Artículo 14 del Tratado constitutivo de la Comunidad Europea[16].

En ella se regulan aspectos precisos de este sector, como por ejemplo lo relativo a la facturación desglosada, la presentación y restricción de la identificación de la línea de origen

---

[10] Artículo 1.2 de la Directiva.

[11] Debemos recordar que en derecho comunitario europeo las Directivas no tienen aplicación directa (salvo en casos en que se deban subsanar situaciones patológicas), por lo cual es necesario que los Estados miembros dicten la legislación de transposición, para lo cual cuentan con un determinado margen de maniobra.

[12] Carta de los Derechos Fundamentales de la Unión Europea, *Diario Oficial n° C 364 de 18/12/2000 p. 001 – 0022,* disponible en: http://europa.eu.int/eur-lex/pri/es/oj/dat/2000/c_364/c_36420001218es00010022.pdf

[13] Artículo 7. Respeto de la vida privada y familiar : "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones. "

[14] Artículo 8. Protección de datos de carácter personal : "1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente. "

[15] Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11, Rome, 4.XI.1950, disponible en: http://conventions.coe.int/treaty/en/Treaties/Html/005.htm

[16] Artículo 14 TCE: "1. La Comunidad adoptará las medidas destinadas a establecer progresivamente el mercado interior en el transcurso de un período que terminará el 31 de diciembre de 1992, de conformidad con las disposiciones del presente artículo, de los artículos 15 y 26, del apartado 2 del artículo 47 y de los artículos 49, 80, 93 y 95 y sin perjuicio de lo establecido en las demás disposiciones del presente Tratado.

2. El mercado interior implicará un espacio sin fronteras interiores, en el que la libre circulación de mercancías, personas, servicios y capitales estará garantizada de acuerdo con las disposiciones del presente Tratado.

3. El Consejo, por mayoría cualificada y a propuesta de la Comisión, definirá las orientaciones y condiciones necesarias para asegurar un progreso equilibrado en el conjunto de los sectores considerados. "

y de la línea conectada, los datos de localización distintos de los datos de tráfico, el desvío automático de llamadas, las guías de abonados, las comunicaciones no solicitadas, etc.[17]

En la presente nota haremos referencia a uno de los temas mas debatidos durante el proceso de adopción de la Directiva, cual es la regulación de los datos de tráfico, dada la sensibilidad del tema respecto de la protección de ciertas libertades fundamentales y la cada vez mas acentuada presión por parte de algunos sectores respecto de la conservación de los mismos como una fuente de información relevante en la lucha contra el cyberdelito y el terrorismo. Nos referiremos pues a la delimitación conceptual, al principio general de aplicación y a los casos en los que se autoriza su procesamiento. Consideraremos, a su vez, la situación actual respecto de la retención y preservación de los datos de tráfico, un tema clave en el cual se refleja cómo, lo acontecido el 11 de septiembre de 2001 en EEUU, incrementó el debate sobre el modo en que deben equilibrarse ciertos intereses políticos que pueden entrar en tensión, en este caso, la seguridad y la salvaguarda de determinados derechos fundamentales.

2. La regulación de los datos de tráfico en la Unión Europea

2.1. Concepto

Si bien en el sistema de telefonía vocal es muy fácil identificar cuáles son los datos de tráfico, ya sea por exclusión, es decir, aquellos que no son datos de contenido, o por enumeración, es decir, el número de teléfono de la persona que llama, el de la persona que es llamada y la duración del llamado, en las comunicaciones electrónicas la conceptualización presenta ciertas dificultades. Por ejemplo, la separación entre contenido y datos de tráfico puede encontrarse, en un cierto punto, desdibujada[18]. La Directiva define los datos de tráfico como "cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma"[19].

---

[17] Resulta interesante reflexionar sobre cuál es el efecto de esta nueva Directiva sobre las Decisiones de Adecuación adoptadas por la Comisión Europea respecto de terceros países. Recientemente se ha emitido un documento de esta especie respecto de la República Argentina, en el cual se declara que nuestra legislación presenta una protección adecuada de los datos personales respecto de la legislación de la UE en la materia. La consecuencia directa de ello es que los datos personales pueden ser transferidos libremente desde la UE a la Argentina para su posterior tratamiento. No obstante, en la Decisión no se hace referencia a la legislación especial, como es el caso de la Directiva 2002/58/CE. La pregunta es entonces: ¿deberán los países que cuentan con tales Decisiones (además de Argentina, Suiza, Hungría, parcialmente Canadá y parcialmente EEUU -Safe Harbour-) adaptar su legislación especial de modo adecuado al de la UE para mantener el status descripto en ellas? No desarrollaremos este tema en el presente artículo, dado que implicaría hacer un análisis integral de la Directiva 2002/58/CE, ahondar en las diferencias respecto de la Directiva general, y evaluar si esas diferencias son susceptibles de influenciar el nivel de adecuación de los terceros países que no cuentan con ellas, lo cual excede el objetivo del presente trabajo. Sobre la Decisión de Adecuación respecto de Argentina ver: María Verónica PEREZ ASINARI "El Mercosur y la Decisión de la Comisión Europea sobre la adecuación de la legislación argentina en materia de protección de datos personales. ¿Se debe pensar en una solución a nivel regional?", a publicarse en *Revista de Derecho Internacional y del Mercosur*, Editorial La Ley, 2003.

[18] Ian HOSEIN y Alberto ESCUDERO PASCUAL "Understanding Traffic Data...", *op. cit.*

[19] Atículo 2.b de la Directiva 2002/58/CE.

La extensión de este concepto no se encuentra delimitada. El Considerando 15 de la Directiva parece emprender un discurso meramente ejemplificativo: "Una comunicación puede incluir cualquier dato relativo a nombres, números o direcciones facilitado por el remitente de una comunicación o el usuario de una conexión para llevar a cabo la comunicación. Los datos de tráfico pueden incluir cualquier conversión de dicha información efectuada por la red a través de la cual se transmita la comunicación a efectos de llevar a cabo la transmisión. Los datos de tráfico pueden referirse, entre otras cosas, al encaminamiento, la duración, la hora o el volumen de una comunicación, al protocolo utilizado, a la localización del equipo terminal del remitente o del destinatario, a la red en que se origina o concluye la transmisión, al principio, fin o duración de una conexión. También puede referirse al formato en que la red conduce la comunicación".

Una ejemplificación que es, no obstante, lo suficientemente ilustrativa como para permitirnos comprender que se trata de una cuestión de alta sensibilidad para la protección de la intimidad, de los datos personales y de la confidencialidad de las comunicaciones. De modo que la mayor extensión del concepto es directamente proporcional al riesgo que representa para la protección de los derechos enunciados. En efecto, los datos de tráfico en el ámbito de las comunicaciones electrónicas son aquellos datos que necesitan los protocolos de Internet para efectuar una transmisión correcta entre el emisor y el destinatario. Se trata de información otorgada por el emisor (por ejemplo: Dirección de correo electrónico del destinatario, URL, etc.) e información generada automáticamente durante el procesamiento de una comunicación electrónica (por ejemplo: dirección IP[20], routers, etc.)[21]. Estos datos son susceptibles de revelar información respecto del usuario de Internet como las personas con las cuales se comunica, los sitios web que visita, la duración y asiduidad de la misma, los documentos que baja, los productos que compra, el lugar donde se encuentra, la lengua que habla, etc., con lo cual ¿podemos identificar aquí datos de contenido?

Como señalamos, la extensión del concepto será dada por la legislación nacional, lo que representa una probabilidad de afectación al mercado interior por poder crear obstáculos para la libre prestación de servicios, ya que, por ejemplo, los consumidores serán proclives a contratar con proveedores de servicios de comunicaciones electrónicas localizados en Estados miembros cuya legislación sea mas respetuosa del derecho a la intimidad, a la protección de los datos personales y a la confidencialidad de las comunicaciones (es decir, cuya legislación adopte un concepto restrictivo de datos de tráfico)[22].

---

[20] En la UE la dirección IP es considerada como un dato personal, lo cual surge de una interpretación conjunta del articulo 2(a) de la Directiva general y el Considerando 26 de la misma. Ver: Article 29 Data Protection Working Party, *Working Document: Privacy on the Internet –An integrated EU Approach to On-line Data Protection*, adoptado el 21 de Noviembre de 2000, WP 37. La autoridad belga de protección de datos personales se ha expedido respecto de ello en *"Avis d'iniciative concernant la compatibilité de la recherche d'infractions au droit d'auteur commises sur Internet avec les dispositions juridiques protégeant les données à caractère personnel et les telecommunications",* Numéro de rôle 44/2001. Allí, la autoridad evalúa la legalidad de ciertas actividades de la IFPI (International Federation of the Phonographic Industry) en Bélgica, en utilización de un sistema de Digital Copyright Management.

[21] Ver: Article 29 Data Protection Working Party, *Working Document: Privacy on the Internet –An integrated EU Approach to On-line Data Protection*, 21 de noviembre 2000, WP 37.

[22] Recordemos que en el Considerando 9 de la Directiva se lee: "Los Estados miembros, los proveedores y usuarios afectados y las instancias comunitarias competentes deben cooperar para el establecimiento y el desarrollo de las tecnologías pertinentes cuando sea necesario para aplicar las garantías previstas en la presente Directiva y teniendo especialmente en cuenta el objetivo de reducir al mínimo el tratamiento de los datos personales y de tratar la información de forma anónima o mediante seudónimos cuando sea posible." La

Por otra parte, podemos preguntarnos específicamente acerca del significado de la frase "dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas", ¿se refiere sólo a los datos "necesarios" para la conducción? En el Artículo 5.1 se establece el principio de confidencialidad de los datos de tráfico, prohibiendo cualquier tipo de intervención o vigilancia de los mismos, determinando *in fine*: "el presente apartado no impedirá el almacenamiento técnico *necesario* para la conducción de una comunicación, sin perjuicio del principio de confidencialidad"[23].

En el Artículo 6.1 se establece: "Sin perjuicio de lo dispuesto en los apartados 2, 3 y 5 del presente artículo y en el apartado 1 del artículo 15, los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público deberán eliminarse o hacerse anónimos cuando ya no sea *necesario* a los efectos de la transmisión de una comunicación"[24].

En el Considerando 26 se lee "Los datos relativos a los abonados que son tratados en las redes de comunicaciones electrónicas para el establecimiento de conexiones y la transmisión de información contienen información sobre la vida privada de las personas físicas, y afectan al derecho de éstas al respeto de su correspondencia, o se refieren a los intereses legítimos de las personas jurídicas. Dichos datos sólo deben poder almacenarse en la medida en que resulten *necesarios* para la prestación del servicio, para fines de facturación y para los pagos de interconexión, y durante un tiempo limitado. (...)"[25].

Por medio de estas referencias podemos inferir que la necesidad debe evaluarse, entonces, en un doble aspecto: tiempo y tipo de datos, y dependiendo de la finalidad de que se trate: conducción de la comunicación o facturación. Con lo cual podríamos concluir que los datos de tráfico que pueden almacenarse, en principio, son aquellos técnicamente necesarios para esas dos finalidades y sólo durante el tiempo necesario para cumplirla.

No obstante, insistimos en que para los otros tratamientos permitidos, que describiremos *infra*, se deberá estar a la extensión dada por el legislador nacional, dentro del marco del artículo 2.1. de la Directiva[26].

---

referencia al principio de "minimización de datos" se repite en el Considerando 30 de la Directiva: "Los sistemas para el suministro de redes y servicios de comunicaciones electrónicas deben diseñarse de modo que se limite la cantidad de datos personales al mínimo estrictamente necesario. (...)". El concepto de datos de tráfico puede depender del diseño de una determinada herramienta o arquitectura, es decir, de cuáles son los datos que los protocolos tratan para conducir la comunicación. Dependiendo de la arquitectura se pueden tratar más o menos datos de forma automática o *by default*.

[23] Énfasis agregado por nosotros.

[24] Énfasis agregado por nosotros.

[25] Énfasis agregado por nosotros.

[26] En 2001, la Comisión Europea realizó una reunión de expertos para debatir acerca de la retención de los datos de tráfico, en el contexto del cyberdelito, en el anexo II a la nota de discusión se enumeran, de modo no exhaustivo, los datos tratados en el contexto de Internet, a saber: "(1) PCs: copies of e-mails sent and received, book-marks, history of web-sites visited, cookies accepted and refused, cache copies of web-data, user Ids and passwords; (2) Network Access Systems (NAS) (dial up services): access logs specific to authentication and authorization servcers, such as TACACS+ or RADIUS used to control acces to IP routers or network access servers, date and time of connection of client to server, User ID, assigned IP address, NAS IP address, number of

2.2. Principio general: confidencialidad de los datos de tráfico

El principio general de aplicación respecto de los datos de tráfico se encuentra expresado en el Artículo 5 de la Directiva, el cual reza: "1. Los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el apartado 1 del artículo 15. El presente apartado no impedirá el almacenamiento técnico necesario para la conducción de una comunicación, sin perjuicio del principio de confidencialidad".

Se establece así la obligación de confidencialidad respecto de los datos de tráfico, los cuales no podrán ser objeto de almacenamiento o cualquier tipo de intervención o vigilancia salvo el consentimiento del usuario o salvo que proceda la excepción establecida en el Artículo 15.1. Recordemos que el consentimiento debe cumplir los requisitos descriptos en la Directiva general[27]. Tampoco se impedirá el almacenamiento necesario para el ruteo de la información.

Si bien la presente Directiva no se aplica a las redes privadas, por ejemplo una Intranet, ello no deja ese sector desprotegido en cuanto a la confidencialidad y demás obligaciones y derechos, ya que se deberá estar siempre a los principios de la Directiva general.

2.3. Tratamiento de los datos de tráfico: excepciones al principio general

2.3.1. Tratamiento para la transmisión de una comunicación

---

bytes transmitted and received, caller line identification; (3) Email servers: SMTP log, date and time of connection of client to server, IP address of sending computer, message ID, sender e-mail address, receiver e-mail address, status indicator, POP log or IMAP log, date and time of connection of client connected to server, User ID, in some cases identifying information retrieved, file upload and download servers; (4) FTP log: date and time of connection of client to server, IP source address, User ID, path and filename of data object uploaded or downloaded; (5) Web Servers: HTTP log, date and time of connection of client to server, IP source address, operation (types of command), path of the operation, last visited page, response codes; (6) Usenet: NNTP log, date and time of connection of client to server, Protocol process ID, host name, basic client activity (but not the content), posted message ID; (7) Internet relay Chat: IRC log, date and time of connection of client to server, duration of session, nickname used during IRC connection, hostname and/or IP address". EU Forum on Cybercrime, *Discussion Paper for Expert's Meeting on retention of Traffic Data*, 6 de noviembre 2001, disponible en: http://europa.eu.int/information_society/topics/telecoms/internet/crime/wpapnov/index_en.htm , última visita: 25/07/03. Vemos así que la legislación debería otorgar mayor precisión. De por sí, no muchos internautas son conscientes de toda la información que generan al utilizar Internet, es por ello que cualquier tratamiento de la misma debe estar rodeado de garantías legales suficientemente detalladas. Aqui vemos cómo, el principio de neutralidad tecnológica puede dejar lagunas que generan inseguridad jurídica.

[27] Artículo 2(h): "consentimiento del interesado": toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.

En el Artículo 6.1 de la Directiva se regula esta posibilidad (o necesidad), estableciendo, a su vez, la obligación de eliminar o anonimizar los datos de tráfico (ver *supra*) cuando ya no resulten necesarios a efectos de la transmisión de una comunicación.

El momento en que termina la transmisión deberá determinarse teniendo en cuenta las especificidades técnicas del servicio de que se trate. Así, el Considerando 27 ejemplifica del siguiente modo: "El momento exacto en que finaliza la transmisión de una comunicación, tras el cual los datos de tráfico deberán eliminarse salvo a efectos de facturación, puede depender del tipo de servicio de comunicaciones electrónicas que se suministre. Por ejemplo, para una llamada de telefonía vocal la transmisión finalizará en cuanto uno de los usuarios interrumpa la conexión; para el correo electrónico la transmisión finaliza en cuanto el destinatario recoge el mensaje, en general del servidor de su proveedor de servicios". A su vez, el Considerando 28 agrega que "[l]a obligación de eliminar datos de tráfico o de hacerlos anónimos cuando ya no se necesiten para la transmisión de una comunicación no entra en conflicto con procedimientos existentes en Internet como la prelectura en soporte rápido (caching), en el sistema de nombres de dominio, de direcciones IP o el caching de una dirección IP vinculada a una dirección física, o a la utilización de información relativa al usuario para controlar el derecho de acceso a redes o servicios"[28].

Las personas legitimadas a tratar los datos de tráficos se encuentran enunciadas en el Artículo 6.5: "Sólo podrán encargarse del tratamiento de datos de tráfico, de conformidad con los apartados 1, 2, 3 y 4, las personas que actúen bajo la autoridad del proveedor de las redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público que se ocupen de la facturación o de la gestión del tráfico, de las solicitudes de información de los clientes, de la detección de fraudes, de la promoción comercial de los servicios de comunicaciones electrónicas o de la prestación de un servicio con valor añadido, y dicho tratamiento deberá limitarse a lo necesario para realizar tales actividades".

Esta referencia, no elimina la posibilidad de subcontratar el tratamiento, respetando siempre el régimen general para ello establecido en la Directiva general[29].

---

[28] La doctrina critica este Considerando por su falta de claridad. Jan DHONT y Karen ROSIER "Directive vie privée et communications électroniques: premiers commentaires", *Revue Ubiquité Droit des technologies de l'information*, FUNDP, DGTIC, CRID, n. 15, abril 2003, p. 37. "Il nous semble que la directive entend indiquer par ces termes, que l'obligation de rendre les données de communications anonymes n'empechêra pas les fournisseurs de services de laisser les technologies visées subsister, quand bien même leur maintien entraînerait la conservation des traces des communications. Cette exception est extrêmement large puisqu'elle autorise cette conservation de données sans limitation de temps, sans garanties et sans droit d'information préalable et d'opposition à celle-ci, sauf à considerer que les dispositions de la directive 95/46/CE s'appliquent aux traitements de données à caractère personnel ainsi mis en œuvre". Nosotros consideramos que en tanto en los procedimientos de mención se traten datos personales, la Directiva 95/46/CE es de aplicación, para cuya identificación no sólo se deberá tener en cuenta el Artículo 2(a) de la misma ["datos personales": toda información sobre una persona física idientificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;], sino también su Considerado 26 [(...)que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona(...)].

[29] Articulo 17.2, .3 y .4 de la Directiva 95/46/EC. Ver el Considerando 32 de la nueva Directiva: "32) Si el proveedor de un servicio de comunicaciones electrónicas o de un servicio con valor añadido subcontrata el tratamiento de datos personales necesario para la prestación de dichos servicios a otra entidad, dicha

2.3.2. Tratamiento a efectos de facturación

En el apartado 2 del Artículo 6 se establece la autorización de este tratamiento y el plazo del mismo: "Podrán ser tratados los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones. Se autorizará este tratamiento únicamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago".

Por lo tanto, si bien se autoriza el tratamiento, se deberá cumplir con las obligaciones que la Directiva general impone al responsable del tratamiento, en particular, en el apartado 4 del mismo Artículo se dispone que "[e]l proveedor del servicio deberá informar al abonado o al usuario de los tipos de datos de tráfico que son tratados y de la duración de este tratamiento a los efectos mencionados en el apartado 2 (...)". A su vez, y *a contrario sensu* de lo establecido en al apartado 3 del mismo artículo y en la segunda parte del apartado 4 (ver *infra*), no se requerirá el consentimiento del abonado para procesar datos de tráfico a efectos de facturación.

No obstante, es preciso considerar que en el contexto de Internet, cada vez se conservan menos datos con el solo fin de facturación. Por un lado, en el caso de utilización de una línea de comunicación de pago por llamada (modem en una línea de teléfono analógico o una línea con adaptador de terminal -ISDN-) el operador de comunicaciones necesita colectar la fecha y la hora de la comunicación, la duración, el número llamado y el número del cliente. Por otro lado, si el cliente usa una conexión DSL, la facturación de esa clase de acceso a Internet se hace mediante el pago de una tarifa plana con un máximo de Mbytes de tráfico por mes. No es necesario, por lo tanto, registrar cada conexión a Internet, sino simplemente contabilizar el volumen de tráfico. Será necesario, sin embargo, identificar el usuario de la linea fija en la cual se activó la conexión DSL. Esos datos son colectados por el operador de telecomunicaciones para fines de facturación. Por encima de ello, se debe considerar al proveedor de acceso a Internet, quien ofrecerá conectividad (rutaje de los paquetes IP en la red) y una dirección IP.

El plazo de conservación lo determina el derecho nacional. Se han detectado divergencias que podrían atentar contra el mercado interior y los derechos garantizados. El Grupo de Trabajo del Artículo 29 ha señalado que el período de conservación a efectos de facturación no deberá exceder los 3 a 6 meses, salvo en los casos de litigio, en los cuales se podría conservar por un período superior[30]. El plazo debe siempre calcularse teniendo en cuenta el Artículo 6.1(e) de

---

subcontratación y el tratamiento de datos subsiguiente deben cumplir plenamente los requisitos relativos a los responsables y a los encargados del tratamiento de datos personales que establece la Directiva 95/46/CE. Si la prestación de un servicio con valor añadido requiere que los datos de tráfico o de localización sean transmitidos por un proveedor de servicios de comunicaciones electrónicas hacia un proveedor de servicios con valor añadido, los abonados o usuarios a los que se refieran dichos datos deben asimismo estar plenamente informados sobre dicha transmisión antes de dar su consentimiento al tratamiento de los datos".

[30] Article 29 Data Protection Working Party, *Opinion 1/2003 on the storage of traffic data for billing purposes*, 29 de enero 2003, WP 69. En otro documento, el Grupo de Trabajo puntalizaba los diferentes plazos existentes en determinados Estados miembros en 1999, lo cual es significativo mencionar: en Alemania, los operadores de telecomunicaciones pueden conservar datos de tráfico a efectos de facturación por un período de 80 días; en Francia, el plazo varía, de acuerdo al status del operador, entre 1 y 10 años; en el Reino Unido, si bien una

la Directiva general[31], y también, que los datos conservados para esa finalidad no deben ser utilizados para otra, salvo que se cumplan los requisitos señalados en las restantes excepciones al principio de confidencialidad y eliminación o anonimización.

2.3.3. Tratamiento a fines de promoción comercial o prestación de servicios con valor añadido

A su vez, existe otro tipo de tratamiento de datos de tráfico autorizado, el cual es regulado en el Artículo 6.3: "El proveedor de un servicio de comunicaciones electrónicas disponible para el público podrá tratar los datos a que se hace referencia en el apartado 1 para la promoción comercial de servicios de comunicaciones electrónicas o para la prestación de servicios con valor añadido en la medida y durante el tiempo necesarios para tales servicios o promoción comercial, siempre y cuando el abonado o usuario al que se refieran los datos haya dado su consentimiento. Los usuarios o abonados dispondrán de la posibilidad de retirar su consentimiento para el tratamiento de los datos de tráfico en cualquier momento."

Ejemplos de servicios de valor anadido son las recomendaciones sobre las tarifas menos costosas, orientacion vial, información sobre tráfico, pevisiones meteorológicas o información turística.[32]

En este caso, el consentimiento deberá obtenerse sólo luego de haber informado al abonado o al usuario acerca de los tipos de datos de tráfico que son tratados y la duración de este tratamiento.

2.3.4. Otras excepciones

En el Artículo 6.5 se extiende a su vez la posibilidad de procesar datos de tráfico a efectos de detección de fraudes y control técnico (ver *supra*). El Considerando 29 refuerza estas finalidades, entre otras, a saber: "De ser necesario, el proveedor del servicio puede tratar, en casos concretos, los datos de tráfico relacionados con los abonados y usuarios, a fin de

---

factura puede ser controvertida durante 6 años, los operadores conservan los datos de tráfico por un período de 18 meses; en Bélgica los operadores conservan los datos durante 3 meses; en Noruega, el período es de 14 días. Article 29 Data Protection Working Party, *Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes*, 7 de septiembre 1999, WP 25. En estos 4 años transcurridos desde la adopción de la Recomendación que citamos, esos plazos pueden haber variado, en Bélgica, por ejemplo, se dictó una ley de criminalidad informática que obligaría a los operadores a retener los datos de tráfico por un período mínimo de 12 meses. No obstante, dicha ley debe ser reglamentada por un decreto real para ser efectiva, el cual todavía no se ha dictado, habiendo recibido, dicho marco regulatorio, numerosas críticas por parte de la Doctrina belga. Ver: Yves POULLET "Lutte contre le crime et/ou vie privée: un débat difficile! A propos de l'alinéa 1er du § 2 de l'article 109ter de la loi belge du 21 mars 1991 introduit par la loi belge du 28 novembre 2000 sur la criminalité informatique", *Revue Ubiquité- Droit des technologies de l'information*, FUNDP, DGTIC, CRID, n. 14, 2002, p. 29-49.

[31] Artículo 6: "1. Los Estados miembros dispondrán que los datos personales sean: (...) e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. (...)"

[32] Considerando 17 de la Directiva.

detectar fallos o errores técnicos en la transmisión de las comunicaciones. El proveedor también puede tratar los datos de tráfico necesarios a efectos de facturación a fin de detectar y frenar el fraude consistente en la utilización sin pago de servicios de comunicaciones electrónicas".

La última excepción contenida en el Artículo 6 es la relativa a la resolución de conflictos, la cual es expresada en el apartado 6, a saber: "Los apartados 1, 2, 3 y 5 se aplicarán sin perjuicio de la posibilidad de que los organismos competentes sean informados de los datos de tráfico con arreglo a la legislación aplicable, con vistas a resolver litigios, en particular los relativos a la interconexión o a la facturación".

2.3.5. Limitación del principio general por motivos de seguridad

La regulación a la cual nos referiremos en este punto ha sido una de las más debatidas durante el proceso legislativo[33]. Aclaramos desde ya que la Directiva que comentamos es un instrumento regulatorio de derechos fundamentales (y de mercado interior), con lo cual, deberá establecer cuáles son los requisitos para poder limitar legalmente los derechos que protege, pero no especificar las limitaciones en sí mismas, ya que para ello se requiere otro tipo de base jurídica en derecho comunitario, o en derecho nacional. Así, en el artículo 15.1 se establece: "Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, (...), cuando tal limitación constituya una medida necesaria, proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE. Para ello, los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea."

En lo que sigue haremos un análisis de los requisitos fijados para que proceda la excepción y luego efectuaremos un acercamiento a la situación europea respecto de la regulación sobre retención y preservación de datos de tráfico.

2.3.5.1. Requisitos para la procedencia de la excepción

Los derechos a la intimidad y a la protección de datos personales no son absolutos. Para que proceda su limitación los requisitos mencionados deben respetarse. La aplicación de los

[33] El Eurodiputado Marco Cappato fue el ponente de la Comisión de Libertades y Derechos de los Ciudadanos, Justicia y Asuntos Interiores encargado de elaborar un informe sobre la propuesta de Directiva, habiendo propuesto algunos cambios al Artículo que comentamos, los cuales no fueron aceptados. Ver : http://www.europarl.eu.int/meetdocs/committees/libe/20010710/439506es.pdf . Ver también: "Open letter to all the Members of the European Parliament. Subject: privacy in the electronic communications (Cappato report), disponible en : http://www.radicalparty.org/privacy/open_lett_cappato_28052002.doc, última visita 25/07/03.

mismos es acumulativa[34], por lo tanto se requiere de se cumplan todos ellos, es decir, la restricción a las ganartías deberá estar determinada en "medidas legales", y deberá ser "necesaria, proporcionada y apropiada en una sociedad democrática".

El primer requisito implica que las limitaciones deberán constar en un texto con carácter de ley (no admitiéndose un Código de conducta, un documento interno, etc.) de modo que provea garantías en contra de arbitrariedades[35], sea accesible a la persona concernida y previsible en cuanto a sus efectos[36]. La "necesidad" implica la inexistencia de otra medida menos violatoria del derecho garantido por la Directiva. Las evaluaciones de necesidad revisten un carácter fáctico, de indagación de la realidad. La "proporcionalidad" requerirá que, al adoptar la medida legislativa en cuestión, el Estado demuestre que la misma obedece a una "necesidad social imperativa", y que la medida adoptada no excede lo necesario para paliar la problemática invocada[37], es decir, el grado de limitación del derecho debe ser proporcional a la finalidad perseguida. Por último, la "pertinencia" se refiere al tipo de medida adoptada, a la naturaleza de la misma y su relación con la finalidad perseguida.

Si bien la correcta aplicación de estos principios deberá ser evaluada por el juez caso por caso, corresponde al legislador nacional o comunitario hacer el análisis del cumplimiento de los mismos antes de proceder a la adopción de las medidas limitativas que respondan a intereses legítimos, como la lucha contra el cyberdelito. No obstante, el monitoreo exploratorio general

---

[34] Siguiendo la jurisprudencia de la Corte Europea de Derechos Humanos en la aplicación del articulo 8.2. del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (en el cual se establece que la restricción al artículo 8.1 sólo podrá operar "de acuerdo con la ley" y cuando sea "necesario en una sociedad democrática"), dada la referencia a dicho instrumento internacional en ambas Directivas. "The interference was not therefore 'in accordance with the law' as required by the second paragraph of Article 8 and there has been a violation of this provision. In these circumstances, an examination of the necessity of the interference is no longuer required", European Court of Human Rights, caso *"P.G. and J.H. v. The United Kingdom"* (Application n. 44787/98), Strasbourg, 25 de septiembre 2001, p. 17. "The Court concludes that the interference cannot therefore be considered to have been 'in accordance with the law' since Swiss law does not indicate with sufficient clarity the scope and conditions of excercise of the authorities' discretionary power in the area under consideration. (...) Having regard to the foregoing conclusion, the Court does not consider it necessary to examine whether the other requirements of paragraph 2 of Article 8 were complied with", European Court of Human Rights, caso *"Amann v. Switzerland"* (Application n. 27798/95), Strasbourg, 16 de febrero 2000, p. 19. Ver también: Vincent COUSSIRAT-COUSTERE "Article 8 § 2", en *La Convention Européenne des Droits de l'Homme. Commentaire article par article*, Dir: Louis PETTITI, Emmanuel DECAUX y Pierre IMBERT, Ed. Economica, 2e Edition, Paris, 1999, p. 323-351.

[35] European Court of Human Rights , caso *"P.G. and J.H. v. The United Kingdom"* (Application n. 44787/98), Strasbourg, 25 de septiembre 2001, p. 17.

[36] European Court of Human Rights, caso *"Amann v. Switzerland"* (Application n. 27798/95), Strasbourg, 16 de febrero 2000, p. 17; caso *"Rotaru v. Romania"* (Application n. 28341/95), Strasbourg, 4 de mayo 2000.

[37] Article 29 Data Protection Working Party, *Recommendation 3/97 on Anonymity on the Internet*, WP 6, 3 de diciembre 1997, page 5. Ver también: Article 29 Data Protection Working Party, *Recommendation 3/99 on The preservation of traffic data by Internet Service Providers for law enforcement purposes*, 7 de septiembre 1999. Article 29 Data Protection Working Party, *Opinion 4/2001 on The Council of Europe 's Draft Convention on Cyber-crime*, WP 41, 22 de marzo 2001. Article 29 Data Protection Working Party, *Opinion 9/2001 on The Commission Communication on 'Creating a safer information society by improving the security of information infrastructures and combating computer-related crime*, WP 51, 5 de noviembre 2001.

y a gran escala de las comunicaciones, por ejemplo, no cumple, en principio, con el requisito de proprocionalidad[38].

2.3.5.2. Retención y preservación de datos de tráfico

Debemos diferenciar los conceptos de "retención" y "preservación" brevemente. La "retención" es realizada *ex ante*, de modo sistemático y por un período de tiempo determinado. La "preservación" es realizada *ex post*, luego de que el evento en disputa ha sucedido o al tener sospecha fundada de que pueda suceder, con orden judicial, y a su vez por un periodo determinado, pudiendo incluir datos de contenido[39].

Los datos de tráfico son muchas veces utilizados por las fuerzas del orden en las investigaciones criminales de delitos cometidos en Internet[40], ya sea de delitos informáticos propiamente dichos (hacking, spoofing, etc.) o perpetrados por delincuentes que utilizan Internet como medio (pornografía infantil, lavado de dinero, etc.). La lucha contra el cyberdelito es un objetivo legítimo e incluído dentro del programa político de la UE[41]. La conservación y utilización de los datos de tráfico a ese fin, sin embargo, debe realizarse respetando las garantías señaladas en el punto anterior para prevenir abusos respecto de las

[38] Yves POULLET "Lutte contre le crime et/ou vie privée: un débat difficile!..", *op. cit*. Commission de la protection de la vie privée (Bélgica), Avis n. 33/1999 "Projets de loi relatifs à la criminalité informatique" Rapport de MM. De SCHUTTER et POULLET, 13 de diciembre 1999, p. 3, 5, 6, 9. En este documento la autoridad belga de protección de datos personales expresa sus objeciones respecto de determinadas normas del proyecto de ley sobre criminalidad informática. Se analizan los criterios para que proceda la excepción a la ley belga de protección de datos, especialmente el de "proporcionalidad", en los casos concretos en que este principio no es respetado por el (entonces) proyecto de ley de mención. Para el marco jurisprudencial sobre sistemas de monitoreo exploratorios ver: European Court of Human Rights, caso *"Malone v. United Kingdon"* (A/82), 1985; European Court of Human Rights, caso *"Klass and Others v. Germany"* (A/28), 1978.

[39] Este es el tipo de medida regulada en la Convención Europea sobre Cyberdelito, en cuyo Artículo 16.2 se establece que las órdenes de preservación no pueden ser superiores a 90 días. Ver: Convention on Cybercrime, Council of Europe, ETS n. 185, disponible en: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm . Este instrumento no ha recibido aún el número de ratificaciones necesarias para entrar en vigor. Ver también: Article 29 Data Protection Working Party, *Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime,* 22 de marzo 2001, WP 41.

[40] EU Forum on Cybercrime, *Discussion Paper for Expert's Meeting on Retention of Traffic data*, 6 de noviembre 2001 (ver supra). Ver también: *Study on Legal Issues Relevant to Combating Criminal Activities Perpetrated Through Electronic Communications*, Queen Mary, University of London, European Commission Contract No. 70369, disponible en: http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/Study2000/Report.html , última visita 24/07/03.

[41] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime", COM(2000) 890 final, p. 18. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions "Network and Information Security: Proposal for a European Policy Approach", Bruselas, 06.06.2001, COM(2001) 298 final. Commission of the European Communities "Proposal for a Council Framework Decision on attacks against information systems", Bruselas, 19.04.2002, COM(2002) 173 final.

libertades fundamentales y evitar declaraciones de inadmisibilidad de la prueba[42], por ejemplo, por haberse obtenido en violación de esas garantías fundamentales.

En el debate sobre la retención y preservación de datos de tráfico entran en juego diferentes partes interesadas: autoridades de protección de datos personales, agentes de ejecución de la ley o fuerzas del orden, la industria de las comunicaciones electrónicas (operadores), y los consumidores, entre otros. Los operadores, por su parte, temen que una obligación de retención por un tiempo prolongado pueda encarecer notablemente el costo del servicio, dados los gastos generados por esa retención, ya que cada vez es mayor la utilización de tarifas planas en el acceso a Internet, por lo cual conservan menos datos a efectos de facturación. Las asociaciones de consumidores objetan el control exacerbado de sus actividades en la red.

Especialmente luego del 11 de septiembre de 2001, una gran controversia ha rodeado la regulación de la retención de los datos de tráfico por razones de seguridad[43], habiendo iniciativas para extender la obligación de retención tanto a nivel comunitario como interno.

En el ámbito de la UE, un proyecto de Decisión Marco sobre la retención de los datos tráfico y el acceso a esos datos en conexión con investigaciones criminales (tercer pilar[44]) ha sido preparado el año pasado por el gobierno belga. Ese proyecto no fue publicado por la UE. Sin embargo, el mismo se filtró a una ONG defensora de las libertades civiles, *Statewatch*, quien lo publicó en su sitio web.[45] El proyecto de Decisión Marco prevee la obligación de retener

---

[42] El riesgo de inadmisibilidad de la prueba electrónica, como una posible consecuencia de la obtención y manipulación de la misma en violación del derecho fundamental a la intimidad y la legislación de protección de datos personales (que es de orden público) fue debatido en la Conferencia "Collecting and Producing Electronic Evidence in Cybercrime Cases", en el marco del proyecto CTOSE (Cyber Tools On-line Search for Evidence) celebrada en la Universidad de Namur, Bélgica, el 8-9 de mayo de 2003. Url del proyecto CTOSE: http://www.ctose.org , ver "Legal constrains for the protection of privacy and personal data in e-evidence handling" presentación de María Verónica PEREZ ASINARI, disponible en: http://www.ctose.org/info/NamurDocs/Perez%20Asinari.ppt .

[43] Article 29 Data Protection Working Party, *Opinion 10/2001 on the need for a balanced approach in the fight against terrorism*, 14 de diciembre 2001, WP 53.

[44] En el derecho de la UE, el tercer pilar se refiere a la cooperación en justicia y asuntos internos.

[45] Ver: http://www.statewatch.org/news/2002/aug/analy11.pdf, última visita 03/07/03. Ver también: Council of the European Union (CEU), 12198/01, Draft Reply to written question P-1887/01 put by Ilka SCRÖDER on 25.06.2001 concerning "Enfopol 29 plans for retention of communication data", 2 de octubre 2001; CEU, 10358/02, Note, "Draft Council conclusions on information technology-related measures concerning the investigation and prosecution of organised crime", 24 de junio 2002; CEU, 11490/02, Cover Note, "Questionnaire on traffic data retention", 12 de agosto 2002; CEU, 12969/02, Preliminary draft reply to written question P-2503/02 put by Kathalijne BUITENWEG on 05.09.2002 concerning "Proposal for a framework directive on data retention", 11 de octubre 2002; The Danish Presidency, "Press release on the retention of traffic data", disponible en: http://www.eu2002.dk/news/news_read.asp?iInformationID=21663 , última visita 03/07/03. The Danish Presidency, "Speaking notes concerning the Danish Presidency of the European Union. Police and judicial co-operation", disponible en: http://www.eu2002.dk/news/upload/JSC20570200273162639.doc , última visita 03/07/03. El proyecto de Decisión Marco tuvo una amplia repercución en la prensa europea: "L'Europe veut allonger le délai de conservation des données de connexion", *Le Monde*, 28.08.02, disponible en: http://www.lemonde.fr/article/0,5987,3416--288412-0,00.html , última visita 31/10/02. "Privacy fear over plan to store email", *The Guardian*, 20.08.02, disponible en: http://www.guardian.co.uk/Print/0,3858,4484984,00.html , última visita 31/10/02.

ciertas categorías de datos de tráfico por un período mínimo de 12 meses y máximo de 24 meses.

El Grupo de Trabajo del Artículo 29 ha emitido un documento debido a sus preocupaciones sobre ciertas propuestas del trecer pilar[46] del derecho de la UE que podrían resultar en la obligación de retener sistemáticamente y de modo exploratorio los datos de tráfico concernientes a todo tipo de comunicaciones por un perídodo de un año o más con fines de ejecución de la ley[47]. La Opinion insiste:

> "Por lo tanto, cuando en casos específicos se deban retener datos de tráfico, debe haber una necesidad demostrable, el período de retención debe ser tan corto como sea posible y la práctica debe estar claramente regulada por la ley, de manera que proporcione suficientes salvaguardias frente a un acceso ilegal o cualquier otro abuso. Una retención sistemática de todas las clases de datos de tráfico por un período de un año o más sería claramente desproporcionada y, por lo tanto, inaceptable en todo caso".

A nivel nacional, se han dictado leyes, también controvertidas, obligando a los operadores a "retener" datos de tráfico por extensos períodos. En España, al transponer la Directiva 2000/31/CE sobre comercio electrónico al derecho interno se "aprovechó" la oportunidad para establecer que "[l]os operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos deberán retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un sevicio de la sociedad de la información por un máximo período de doce meses, en los términos establecidos en este artículo y en su normativa de desarrollo"[48].

No obstante, numerosas preguntas quedan aún sin respuesta. ¿Cuál es la protección que se le dará a los datos de tráfico que revelen información sensible (como la visita a determinados sitios web que permitan inferir la orientación religiosa, filosófica, política, sexual, datos relativos a la salud del usuario, etc.? ¿Cumple con los requisitos de proporcionalidad o necesidad del mismo modo un período extenso de retención legislado para luchar contra delitos que revisten una gravedad diversa (violación de derechos de propiedad intelectual y pronografía infantil, por ejemplo)? ¿Cómo se asegurará la seguridad de esos datos? ¿Quedarán, los datos recabados, bajo el control de los operadores, pasarán a las fuerzas del orden, o a terceros (*Trusted Third Parties*)? ¿Cómo se asegurará la autenticidad de los datos para que puedan ser considerados como prueba válida en los Tribunales (los datos digitales son de extrema volatilidad y muy fáciles de ser alterados -ya sea por falta de profesionalidad de quien los manipula o exceso de destreza para destruir la prueba intencionalmente-)?

---

[46] En clara referencia al Proyecto de Decisión Marco que mencionamos *supra*.

[47] Grupo de Trabajo del Artículo 29, *Dictamen 5/2002 sobre la Declaración de los Comisarios Europeos responsables de protección de datos en la Conferencia Internacional celebrada en Cardiff (9-11 de septiembre de 2002) sobre la retención sistemática obligatoria de datos sobre tráfico de telecomunicaciones,* 11 de octubre 2002, WP 64.

[48] Artculo 12, Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, BOE num. 166. España no está sola en esta tendencia, por ejemplo, Bélgica (*Loi du 28 novembre 2000 relative à la criminalité informatique*. Moniteur Belge, 03.02.2001) y Francia (*Loi sur la securité quotidienne*. Journal Officiel. Numéro 266 du 16 Novembre 2001) también han dictado leyes que fijan el plazo de retención en 1 año, aunque sus decretos reglamentarios todavía no han sido adoptados.

¿Cómo se solucionarán los problemas para el mercado interior europeo derivados de la divergencia de los plazos nacionales de retención o de la extensión del concepto de datos de tráfico o la determinación de quién se hará cargo de los costos de retención que excedan las prácticas habituales de los operadores? Se trata, pues, de un debate abierto, el cual debe ser guiado en la consideración de los principios descriptos. No obstante, mientras estas dudas (entre otras) no se disipen, resultaría extraño que pudiera invocarse el cumplimiento de los mismos.

3. A modo de colofón

Si bien la presente nota es un acercamiento marcadamente sintético al tema en cuestión, podemos ver cuáles son los riesgos generados por el tratamiento de los datos de tráfico para la protección de los derechos fundamentales, en especial la intimidad, los datos personales y el secreto de las comunicaciones. Se debe atender, por lo tanto, de modo meticuloso al equilibrio de intereses contrapuestos de modo que las garantías jurídicas no se vean limitadas más alla de lo estrictamente necesario, de modo proporcional y apropiado, basándose en leyes que describan los procedimientos a seguir y con el pertinente control judicial.

En cuanto a las iniciativas del tercer pilar, es de esperar que en el caso que prosperen se basen estrictamente en las condiciones establecidas tanto en la Convención Europea para la Protección de los Derechos Humanos y Libertades Fundamentales, en la Carta de la UE de Derechos Fundamentales y la legislación de protección de datos, donde se regulan las excepciones a la aplicación de sus preceptos, sin olvidar uno de los principios jurídicos más básicos: las excepciones son de interpretación restrictiva.

Vemos también cómo se aplican los principios generales establecidos en la Directiva 95/46/CE a un caso particular, como es el de los datos de tráfico. Sin embargo, debemos señalar que determinados aspectos que pueden afectar al mercado interior europeo, como por ejemplo la extensión del concepto de datos de tráfico, o de los intereses legítimos de las personas jurídicas, no han sido lo suficientemente aclarados, y el margen de maniobra que se deja a los Estados miembros podría derivar en obstáculos a la libre circulación de datos personales y otras libertades del mercado interior. Este tipo de conflictos deberán prevenirse en el Mercosur cuando se encare la necesaria tarea de armonización de la legislación relativa a la protección de datos personales.